Identity Theft: Consumers, Creditors & Criminals
Civil and Criminal Enforcement

Program Co-Sponsors
The State Bar of California Business Law Section
Financial Institutions Committee
and
Beverly Hills Bar Association

12:00 Noon, November 12, 2002
Offices of Manatt, Phelps & Phillips LLP
Trident Center, East Tower
11355 Olympic Boulevard
Los Angeles, California

Over the past two years, California's legislature has adopted a number of laws that expand the remedial provisions for Californians whose personal identifying information has been unlawfully used by others. These laws, although not forming any comprehensive or coordinated plan, serve as tools the consumer may utilize to protect and restore creidt and personal identifying information. While some aspects of this paper touch on consumer privacy, the primary purpose is to offer a synopsis of California and federal laws specifically dealing with identity theft.

California's Criminal Identity Theft Provisions

Effective January 1998, California adopted criminal provisions[1] dealing with the unlawful use of "personal identifying information."[2] That law makes it unlawful for a person to willfully obtain personal identifying information of another without that person's consent and to use that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services or medical information, or with intent to use that information to defraud another person.[3] Upon conviction, the unauthorized person (ID thief) may be punished either by (1) imprisonment in county jail for up to one year, by a fine not to exceed $1,000, or both imprisonment and fine, or (2) by imprisonment in state prison or a fine up to $10,000, or both imprisonment and fine.[4] When two or more persons receive a felony conviction for conspiring to commit identity theft, the court may impose a fine of up $25,000.[5]

---

[1] Laws 1997, Ch. 768 (A.B. 156) amended by Laws 1998, Ch. 488 (S.B. 1374).
[2] "Personal identifying information" means the person's name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, or credit card number. Cal. Pen. Code § 530.5(b). The definition was expanded by Laws 2002, Ch. 254 (S.B. 1254), to include health insurance ID, taxpayer ID, school ID, checking account number, PIN or password, alien registration number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voice print, retina or iris image, or other unique physical representation, unique electronic data including identification number, address or routing code, telecommunication identifying information or access device, information from a birth or death certificate.
[3] Cal. Pen. Code § 530.5(a), (d).
[4] *Id.*
[5] Penal Code § 182, as amended by Laws 2002, Ch. 907 (A.B. 1155).

Any person who obtains, or assists another person in obtaining a driver's license, identification card, vehicle registration certificate, or any other official document issued by the Department of Motor Vehicles with knowledge that the person obtaining the document is not entitled to it is guilty of a misdemeanor, and is punishable by imprisonment in a county jail for up to one year, or a fine of up to $1,000 or both.[6]

A key provision of the criminal statutes added is the power it gives individual victims to pursue remedies to the damage done as a result of the theft. One of the remedies involves the ability to have local law enforcement initiate an investigation. A person who has learned or suspects that personal identifying information has been unlawfully used by another may have the local law enforcement initiate an investigation by contacting the agency that has jurisdiction over the victim's residence (city or county police departments) and by filing a police report. The local law enforcement agency where the victim resides may refer the matter to the law enforcement agency where the suspected crime was committed for investigation.[7]

Another key provision effective January 1, 2002,[8] is the ability to obtain information about the victim's ID theft from creditors and other providers. If the victim discovers that an application in his or her name for a loan, credit line or account, credit card, charge card, utility service, or commercial mobile radio service has been filed with a creditor or provider, or that an account in the person's name has been opened with a financial institution or utility or commercial mobile radio service provider by an unauthorized person, the victim may present a copy of the police report that was filed pursuant to Cal. Penal Code Section 530.6, along with identifying information in the "categories of information that the unauthorized person used to complete the application or to open the account," and obtain information related to the loan or account, including a copy of the application and a record of the transactions or charges. The creditor must, if the victim requests it, inform him or her of the categories of identifying information that the unauthorized person used to complete the application or open the account.[9] The creditor, financial institution or provider must provide this information including copies of forms without charge within 10 business days of receipt of the person's request and submission of police report and identifying information.[10]

The victim also has the ability to petition the court to render an expedited judicial determination of his or her innocence where the perpetrator has been arrested for or convicted of the ID theft, or where the victim's identity has been mistakenly associated with a record of criminal conviction.[11] The California Department of Justice has established a database of individuals who have been victims of ID theft that can be accessed by criminal justice agencies, victims, and individuals and agencies representing or authorized by victims.[12]

---

[6] New Penal Code § 529.7, added by Laws 2002, Ch. 907 (A.B. 1155). It is surprising that no specific law existed prior to this to punish those who aid in obtaining fake drivers' licenses, a distinct problem in California for years.
[7] Cal. Pen. Code § 530.6(a).
[8] Laws 2001, Ch. 493 (S.B. 125).
[9] Cal. Pen. Code § 530.8, as amended by Laws 2002, Ch. 254 (S.B. 1254).
[10] *Id.*
[11] Cal. Pen. Code § 530.6(b), as amended by Laws 2002, Ch. 851 (A.B. 1219).
[12] Cal. Pen. Code § 530.7(c). A toll-free telephone number to provide access to the database is available: 888-880-0240. Cal. Pen. Code § 530.7(d). In order to be included in the database, the victim must submit a court order, a full set of fingerprints, and any other information the Department of Justice requires. Cal. Pen. Code § 530.7(a). Tips and registry application forms are at: www.caag.state.ca.us; click on "Programs and Services," and under "Criminal Justice," click on "Identity Theft."

These criminal provisions form the cornerstone of other civil actions the victim may take under California law, discussed below.

California's Civil Identity Theft Law

Effective January 1, 2002,[13] California adopted a new title to the Civil Code recognizing remedial rights for victim's of identity theft. The bill also added some surprise provisions to, and strengthened by amending other provisions of, the Consumer Credit Reporting Agencies Act, discussed in more detail under *Problems with Address Verification* and *Added Responsibilities for Credit Reporting Agencies*, below.

First, the new law gives a person who is a victim of identity theft the right to bring an action against a "claimant', i.e., one who has or purports to have a claim for money or an interest in property in connection with a transaction procured through identity theft, or to file a cross-complaint if a suit has initiated against the victim.[14] A "victim of identity theft" is a person who had his or her personal identifying information used without authorization by another to obtain credit, goods, services, money or property obtained by identity theft, and filed a police report pursuant to Cal. Penal Code Section 530.6.[15] The victim need only establish that he or she is a victim of identity theft by a preponderance of the evidence.[16]

If the person proves that he or she is a victim of identity theft, the person is entitled to a judgment as follows:

(1) A declaration that he or she is not obligated to the claimant on the claim.

(2) A declaration that any security interest or other interest the claimant had purportedly obtained in the victim's property in connection with that claim is void and unenforceable.

(3) An injunction restraining the claimant from collecting or attempting to collect from the victim on that claim, from enforcing or attempting to enforce any security interest or other interest in the victim's property in connection with that claim, or from enforcing or executing on any judgment against the victim on that claim.

(4) Actual damages, attorney's fees, and costs, and any equitable relief that the court deems appropriate. In order to recover actual damages or attorney's fees, the person must show that he or she provided written notice to the claimant that a situation of identity theft might exist, including, upon written request of the claimant, a valid copy of the police report or the Department of Motor Vehicles investigative report filed pursuant to Cal. Penal Code Section 530.6 at least 30 days prior to the filing of the action or within the cross-compliant.

---

[13] Laws 2001, Ch. 354 (A.B. 655); Cal. Civ. Code §§ 1798.92-1798.97.
[14] Cal. Civ. Code §§ 1798.92(a), 1798.93(a).
[15] Cal. Civ. Code § 1798.92(d). "Personal identifying information" is defined the same as in Cal. Pen. Code § 530.5(b). Cal. Civ. Code § 1798.92(c).
[16] Cal. Civ. Code § 1798.93(b).

(5) Statutory damages of up to $30,000 if the victim establishes by clear and convincing evidence that:

(a) At least 30 days prior to the filing of the action or the cross-complaint, the victim provided written notice to the claimant at the address designated by the claimant for complaints related to credit reporting issues that a situation of identity theft might exist and the basis for that belief.

(b) That the claimant failed to diligently investigate the victim's notification of a possible identity theft.

(c) That the claimant continued to pursue its claim against the victim after the claimant was presented with facts that were later held to entitle the victim to judgment.[17]

The new law provides for a four-year statute of limitations. The action may be brought within four years of the date the person who alleges that he or she is a victim of identity theft knew, or in the exercise of reasonable diligence, should have known of the existence of facts that would give rise to the bringing of the action.[18] The new provisions do not apply to a transaction in which a credit card holder is liable for unauthorized use of a credit card where (i) the amount of the charge is $50 or less, (ii) the card issuer gives adequate notice to the card holder of the unauthorized use, (iii) the card issuer has provided the card holder with a description of a means by which the card issuer may be notified of loss or theft of the card, (iv) the unauthorized use occurred before the card issuer has been notified that an unauthorized use of the card has occurred or may occur as a result of the loss or theft of the card, and (v) the card issuer has provided a method whereby the user of the card can be identified as the person authorized to use it.[19]

Provisions Specific to California Credit Card Issuers

The new California law also helps victims get copies from their credit card account files.[20] Effective January 1, 2002, credit card issuers must provide to a person who is a victim of identity theft, or to the law enforcement officer specified by such person, copies of all application forms or information containing the person's name, address, or other identifying information pertaining to the application filed with the credit card issuer by an unauthorized person.[21] Before providing copies, the card issuer must inform the requesting person of the categories of identifying information that the unauthorized person used to complete the application, and must require the requesting person to provide identifying information in those categories, and a copy of the police report.[22]

Within 10 business days of receipt of the request and a copy of the police report and identifying information, the card issuer must provide without charge copies of all forms and information required.[23]

---

[17] Cal. Civ. Code § 1798.93(c).
[18] Cal. Civ. Code § 1798.96.
[19] Cal. Civ. Code § 1747.10.
[20] Laws 2001, Ch. 493 (S.B. 125).
[21] Cal. Civ. Code § 1748.95(a)(1).
[22] Cal. Civ. Code § 1748.95(a)(2).
[23] Cal. Civ. Code § 1748.95(a)(3).

Before the card issuer provides the copies to a law enforcement officer, the card issuer may require the requesting person provide the card issuer with a signed and dated statement by which the requesting person: (a) authorizes disclosure for a stated period; (b) specifies the name of the agency or department to which the disclosure is authorized; and (c) identifies the type of records that the person authorizes be disclosed. The card issuer must include in the statement to be signed a notice that the person has the right at any time to revoke the authorization.[24]

Provisions Specific to California Finance Lender Licensees

Similar provisions have been adopted for licensees under the California Finance Lenders Law ("CFLL"). Effective January 1, 2002,[25] a person who has been the subject of identity theft, and who has filed a police report[26] has the right to request a CFLL licensee to provide copies of items from the loan file. The CFLL licensee must, within 10 business days of receipt of the person's request, provide to the person, or law enforcement officer, copies of all application forms, and application information containing the person's name, address, or other identifying information pertaining to the application,[27] filed with the CFLL licensee by the unauthorized person.[28] The CFLL licensee must inform the requesting person of the "categories of identifying information that the unauthorized person used to complete the application."

Also, the CFLL licensee has the right to request the person asking for copies to provide identifying information and a copy of the police report.[29]

Before the CFLL licensee provides copies to the law enforcement officer, the CFLL licensee has the right to demand the requesting person provide a signed and dated statement that: (a) authorizes the disclosure for a stated period; (b) specifies the name of the agency or department to which disclosure is authorized; (c) identifies the type of records that are authorized to be disclosed; and (d) contains the notification that the requesting person has the right at any time to revoke the authorization.[30]

Provisions Specific to "Supervised Financial Organizations"

Effective January 1, 2002,[31] upon the request of a person who has obtained a police report concerning that person's identity theft, a supervised financial organization[32] ("SFO") must provide to the person, or to a law enforcement officer specified by the person, copies of all application forms or application information containing the person's name, address, or other identifying information pertaining to the application filed with the SFO by an unauthorized person in violation of the criminal provisions dealing with identity theft.[33]

---

[24] Cal. Civ. Code § 1748.95(b).
[25] Laws 2001, Ch. 493 (S.B. 125).
[26] Pursuant to Cal. Penal Code § 530.6.
[27] Cal. Fin. Code § 22470(a).
[28] In violation of Cal. Penal Code § 530.5.
[29] Cal. Fin. Code § 22470(a).
[30] Cal. Fin. Code § 22470(b).
[31] Laws 2001, Ch. 493 (S.B. 125).
[32] A "supervised financial organization" is a state or federally regulated bank, savings association, savings bank, or credit union, or a subsidiary of any of the foregoing. Cal. Fin. Code § 4000(a)(9).
[33] Cal. Fin. Code § 4002(a)(1).

Before providing the person with copies requested, the SFO must inform the requesting person of the categories of identifying information that the unauthorized person used to complete the application, and must require the requesting person to provide identifying information in those categories, and a copy of the police report.[34] This particular provision, like the one dictated by the CFLL, controls the method by which the apparent truth of the identity of the victim is established with the SFO. The SFO must then provide copies of all forms and information required, without charge, within 10 business days of receipt of the person's request and submission of the required copy of the police report and identification.[35]

Before a supervised financial organization provides copies to a law enforcement officer, the SFO may require the requesting person to provide the SFO with a signed and dated statement by which the person does all of the following: (a) authorizes disclosure for a stated period; (b) specifies the name of the agency or department to which the disclosure is authorized; and (c) identifies the type of records that the person authorizes to be disclosed.[36] The statement to be signed must include a notice that the person has the right at any time to revoke the authorization.[37]

Address Verification Problems

Some ambiguous additions to California's Consumer Credit Reporting Agencies Act accompanied the Identity Theft law. Effective January 1, 2002, any person who used a consumer credit report in connection with a credit transaction, and who discovered that the address on the consumer credit report did not match the address of the consumer requesting or being offered credit, was required to take reasonable steps to verify the accuracy of the consumer's address, by either communicating to the consumer by telephone, or writing to the consumer, to confirm that the credit transaction was not the result of identity theft.[38]

The law was recently amended, effective September 28, 2002.[39] The amendments clarified, somewhat, the requirements for verification, and added some additional responsibilities. Any person who uses a consumer credit report in connection with the approval of credit based on an application for an extension of credit, and who discovers that the address on the credit application does not match, within a reasonable degree of certainty, the address or addresses listed, if any, on the consumer credit report, must take reasonable steps to verify the accuracy of the address provided on the application to confirm that the extension of credit is not the result of identity theft.[40] One might wonder what the real distinction is between the old language (above) and the new language. The differences are important in four respects: First, if a creditor has evaluated the credit of the applicant and has determined that it will not extend credit (adverse action), the additional time and expense of verification need not be undertaken.

[34] Cal. Fin. Code § 4002(a)(2).
[35] Cal. Fin. Code § 4002(a)(3).
[36] Cal. Fin. Code § 4002(b)(1).
[37] Cal. Fin. Code § 4002(b)(2).
[38] Cal. Civ. Code § 1785.20.3(a).
[39] Laws 2002, Ch. 1030.
[40] Cal. Civ. Code § 1785.20.3(a).

Second, the prior language applied to any activity in connection with a consumer credit transaction. Arguably, that could mean collection of an existing account,[41] or in connection with preapproved firm offers of credit. Third, the new language added "a reasonable degree of certainty." A creditor need not worry about minute differences in the address, such as "Drive" instead of "Street" or even some differences in the name of the city, *e.g.*, "Palos Verdes Estates" versus "Palos Verdes Peninsula." Fourth, the creditor has some flexibility in how it confirms that the address discrepancy does not raise red flags that there is an identity theft involved. The creditor is no longer required to either communicate to the consumer by telephone or in writing to confirm that the credit transaction is not the result of identity theft. A creditor may have better and faster means of confirming the identification of an applicant, and is now free to employ those means.

The law as amended still fails to take into account that credit application transactions are, for the most part, handled electronically and processed within seconds without human intervention. Creditors must still rewrite programs and adopt additional steps, costing consumers and companies time and money, to comply with the address verification law. On the positive side, verification of applicant identity has resulted in ferreting out identity thieves, and avoided ruining the credit of innocent consumers.

The 2002 amendments also impact another provision of the address verification law that needed revision. Until September 28, 2002, any person who used a consumer credit report in connection with a credit transaction and who received a "clearly identifiable notification, consisting of more than a tradeline (on a credit report) from a consumer credit reporting agency that information in the report had been blocked pursuant to Cal. Civil Code Section 1785.16 as a result of identity theft," was prohibited from lending money or extending credit without taking reasonable steps to verify the consumer's identity and to confirm that the credit transaction was not the result of identity theft. There do not appear to be any statistics available on the frequency of occurrence of this factual circumstance.

The words "clearly identifiable" and "consisting of more than a tradeline from a consumer credit reporting agency that information in the report has been blocked" pursuant to California Civil Code Section 1785.16[42] have been deleted. The subdivision[43] now refers to "any person who uses a consumer credit report in connection with the approval of credit based on an application for an extension of credit," and simply refers to "notification pursuant to subdivision (k) of Section 1785.16 that the applicant has been the victim of identity theft . . . " Creditors who receive such a notice must not extend credit without taking reasonable steps to verify the consumer's identity.

The strict damages provision in this part of the law is still intact. A consumer who suffers damages as a result of a violation of either of the foregoing provisions by any person is given the right

---

[41] The "extension of credit" does not apply to an increase in an open-end credit plan or any change to or review of an existing credit account. Cal. Civ. Code § 1785.20.3(e).

[42] Cal. Civ. Code § 1785.16(k) provides, in part, if a consumer submits to a credit reporting agency a copy of a valid police report, or a valid investigative report made by a Department of Motor Vehicles investigator with peace officer status, . . . the consumer credit reporting agency must promptly and permanently block reporting any information that the consumer alleges appears on the credit report as a result of identity theft, so that the information cannot be reported. This subdivision and subdivision (*l)* also contain procedures for unblocking information, or errors in blocking information, and reinvestigating and correcting disputed information in this setting. These procedures are in different than those described in "security alerts" and "security freezes."

[43] Cal. Civ. Code § 1785.20.3(b).

to bring an action in court against that person to recover actual damages, court costs, attorney's fees, and punitive damages of not more than $30,000 for each violation, as the court deems proper.[44]

Added Responsibilities for Credit Reporting Agencies

The burden of the many procedural aspects of complying with the California's identity theft laws has fallen most heavily on the shoulders of the credit reporting agencies.[45] Some of the new requirements are duplicative of laws that had been previously adopted (see *"Security Alerts" and "Security Freezes"* below). Other provisions have been temporarily suspended until January 1, 2003, due to the inability of the credit reporting agencies to implement them by the effective date and because the intent of the legislature was that they be effective on a date to coincide with other operative provisions.[46]

Of course, a California consumer has had the right to access the information in his or her credit file for many years. Credit reporting agencies have established procedures for this, and provide certain notices to a consumer of those rights.[47] Effective January 1, 2003, in addition to providing the names and addresses of the sources of information that compile the consumer's credit file, the agency must also provide the telephone numbers identified for customer service for those sources.[48]

Furthermore, the credit reporting agency must disclose the recipients of any consumer credit report that has been furnished for employment purposes within the preceding two-year period, or for any other purpose within the preceding 12-month period.[49] Effective January 1, 2003, in addition to the names and address of the recipients, the agencies must include the telephone number identified for customer service for those recipients.[50] The agency must also disclose a record of all inquiries received by the agency within the preceding 12-month period for transactions not initiated by the consumer[51] and in addition to disclosing the name and address, effective January 1, 2003, must disclose the telephone number identified for customer service for each such person making an inquiry.[52] Resellers or aggregators of consumer credit reports are exempt from certain of these provisions.[53]

In July 1998, the ability to "block" information on a credit report was adopted, provided the consumer had filed a police report under California Penal Code Section 530.6. Starting January 2002, the consumer may also block information based on a valid investigative report made by the Department of Motor Vehicles, provided the investigator has "peace officer" status.[54] If a consumer submits to a credit reporting agency a copy of a valid police report or a valid investigative report filed pursuant to California Penal Code Section 530.6, the credit reporting agency must promptly and permanently block reporting of any information that the consumer alleges appears on his or her report

---

[44] Cal. Civ. Code § 1785.20.3(c).
[45] Laws 2001, Ch. 354 (A.B. 655).
[46] Laws 2002, Ch. 9 (A.B. 1531) referring to Laws 2001, Ch. 236 (A.B. 488) effective January 1, 2003.
[47] Cal. Civ. Code § 1785.10; *see also* Cal. Civ. Code §§ 1785.11.8, 1785.15, 1785.15.1, 1785.17, 1785.19 and 1785.19.5.
[48] Cal. Civ. Code § 1785.10(c).
[49] Cal. Civ. Code § 1785.10(d)(1).
[50] Cal. Civ. Code § 1785.10(d)(2).
[51] Such as for purposes of creditors making "firm offers of credit," Cal. Civ. Code § 1785.20.1.
[52] Cal. Civ. Code § 1785.10(e).
[53] Cal. Civ. Code § 1785.10(f) and (g).
[54] Cal. Civ. Code § 1785.16(k).

as a result of the violation of the identity theft law, so that the information cannot be reported. The credit reporting agency must promptly notify the furnisher of the information that the information has been so blocked. Furnishers of information, and credit reporting agencies, must ensure that information is unblocked only upon a preponderance of evidence establishing the following:

(1) The information was blocked due to a material misrepresentation of fact by the consumer or fraud;

(2) The Consumer agrees that the blocked information, or portions of the blocked information, were blocked in error; or

(3) The consumer knowingly obtained possession of goods, services, or moneys as a result of the blocked transaction(s) or the consumer should have known that he or she obtained possession of goods, services or moneys as a result of the blocked transaction(s).[55]

If blocked information is unblocked pursuant to these rules, the consumer must be promptly notified. In unblocking information pursuant to these rules, furnishers and credit reporting agencies must be subject to their respective requirements regarding the "completeness and accuracy of information."[56]

Also, in unblocking the credit file, the credit reporting agency must comply with the "reinvestigation of dispute" rules,[57] and accept the consumer's version of the disputed information and correct or delete the disputed item when the consumer submits to the credit reporting agency documentation obtained from the source of the item in dispute or from public records confirming that the report was inaccurate or incomplete. The credit reporting agency can refuse to delete the disputed information if, in the exercise of good faith and reasonable judgment, it has substantial reason based on specific, verifiable facts to doubt the authenticity of the documentation submitted and notifies the consumer in writing of that decision, explaining its reasons for unblocking the information and setting forth the specific, verifiable facts on which the decision was based.[58]

Also in 2002, a credit reporting agency must, without a request from the consumer, delete inquiries for credit reports based upon credit requests that the consumer credit reporting agency verifies were initiated as the result of identity theft.[59]

Effective January 1, 2003, the written summary of rights provided to a consumer that receives information from the consumer's credit file from the credit reporting agency must include a new provision informing the consumer of certain rights if that consumer is the victim of identity theft: "If you are a victim of identity theft and provide to a consumer credit reporting agency a copy of a valid police report or a valid investigative report made by a Department of Motor Vehicles investigator with peace officer status describing your circumstances, the following shall apply: (1) You have a right to have any information you list on the report as allegedly fraudulent promptly blocked so that the information cannot be reported. The information will be unblocked only if (A) the information you

[55] Cal. Civ. Code § 1785.16(k).
[56] *See* Cal. Civ. Code §§ 1785.14, 1785.25, 1785.30.
[57] *See* Cal. Civ. Code § 1785.16(a) – (j).
[58] Cal. Civ. Code § 1785.16(*l).*
[59] Cal. Civ. Code § 1785.16.1.

provide is a material misrepresentation of the facts, (B) you agree that the information is blocked in error, or (C) you knowingly obtained possession of goods, services, or moneys as a result of the blocked transactions. If blocked information is unblocked you will be promptly notified. (2) Beginning July 1, 2003, you have a right to receive, free of charge and upon request, one copy of your credit report each month for up to 12 consecutive months."[60]

In addition to the foregoing, effective July 1, 2003, a consumer credit reporting agency must promptly provide to a consumer a statement, written in a clear and conspicuous manner, describing the statutory rights of victims of identity theft under the California Consumer Credit Reporting Agencies Act after the agency has been contacted by telephone, mail, or in person by a consumer who has reason to believe he or she may be a victim of identity theft.[61]

Another addition to the Consumer Credit Reporting Agencies Act created almost as much havoc in the credit industry as the address verification provisions. A creditor is prohibited from selling a consumer debt if the consumer's file with a credit reporting agency is blocked with respect to that debt, or if the consumer provided the creditor with sufficient information in writing that the consumer is not obligated to pay the debt because he or she is a victim of identity theft, for the creditor to have reasonable grounds to determine that the consumer's statement of identity theft is not frivolous.[62] The problem here is that in modern money markets, accounts and transactions are bundled and sold in the secondary market or pooled and securitized. Typically, no credit reports are pulled prior to the consummation of these transactions, so the creditor would never know if the consumer's existing account with that creditor is "blocked" or whether the customer had communicated to the creditor that he or she is a victim of identity theft, or whether if the customer had, if that communication pertained to an identity theft involving that creditor and that account. These problems have been marginally rectified by an amendment effective September 28, 2002. No creditor may sell a consumer debt to a *debt collector, as defined in 15 U.S.C. Sec. 1692a*[63] if the consumer is a victim of identity theft with respect to that debt and the creditor has received notice of that fact from a credit reporting agency that the credit file has been blocked.[64]

Some amendments have also been made to the investigative consumer reports provisions of the Consumer Credit Reporting Agencies Act.[65] Investigative consumer reports are used by prospective employers, current employers, and by insurance companies. These changes mostly deal with providing a copy of the investigative report to the consumer who is the subject of the report except in cases where the employer is in the process of determining whether to discharge an employee engaged in

---

[60] Cal. Civ. Code § 1785.15 as amended by Laws 2002, Ch. 860 (S.B. 1239). The consumer credit reporting agency is obligated to provide the free credit reports (up to 12, one per month following the date of the police report). New Cal. Civ. Code § 1785.15.3, effective July 1, 2003.

[61] New Cal. Civ. Code § 1785.15.3, added by Laws 2002, Ch. 860 (S.B. 1239).

[62] Cal. Civ. Code § 1785.16.2. A sale of the debt to a subsidiary or affiliate of the creditor is allowed. Cal. Civ. Code § 1785.16.2(b).

[63] The Federal Fair Debt Collection Practices Act defines a "debt collector," in part, as any person who uses any instrumentality of interstate commerce or the mails I any business the principal purpose of which is the collection of any debts, or who regularly collects, or attempts to collect, directly or indirectly, debts owed or due or asserted to be owed or due another. Notwithstanding the exclusion provided by subsection (F) [certain exceptions omitted], the term includes any creditor who, in the process of collecting his own debts, uses any name other than his own which would indicate that a third person is collecting or attempting to collect such debts.

[64] Cal. Civ. Code § 1785.16.2 as amended by Laws 2002, Ch. 1030 (A.B. 1068).

[65] Laws 2001, Ch. 354 (A.B. 655).

criminal activity likely to result in loss to the employer,[66] to retaining copies of investigative reports for three years, and to providing for or increasing damages provisions.[67]

"Security Alerts" and "Security Freezes"

Effective July 1, 2002,[68] a California consumer may place a "security alert" in his or her credit report by making a request in writing to or by calling an 800 telephone number (24 hours a day, seven days a week) of the consumer credit reporting agency.[69] A "security alert" notifies a recipient of the credit report that the consumer's identity may have been used without the consumer's consent to fraudulently obtain goods or services in the consumer's name. The alert may remain in place for at least 90 days, and a consumer has a right to request a renewal of the alert.[70]

Effective January 1, 2003, a California consumer may place a "security freeze" on his or her credit report by making a request in writing by certified mail to a consumer credit reporting agency.[71] A "security freeze" prohibits the consumer credit reporting agency, subject to certain exceptions, from releasing the consumer's credit report without the express authorization of the consumer.

The credit reporting agency must place the security freeze within five business days of receiving the written request from the consumer,[72] and within 10 business days, send to the consumer written confirmation of the security freeze. The credit reporting agency must also provide a PIN or password the consumer may use when providing authorization for release of credit information for a specific party or period of time.[73] So long as a security freeze is in place, a credit reporting agency must not change any of the following official information in a credit file without sending a written confirmation of the chance to the consumer within 30 days of the change being posted to the file: name, date of birth, social security umber, and address.[74]

The credit reporting agency may advise a recipient that a security freeze is in place. The person considering an application for which a security freeze has been put into effect may consider the application as "incomplete."[75]

There are certain exceptions to the prohibition on the release of the consumer credit report, among them, to an assignee of a financial obligation owing by the consumer, or a prospective assignee of a financial obligation owing by the consumer in conjunction with the proposed purchase of the financial obligation, or to a person to whom the consumer issued a negotiable instrument, for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract, or negotiable instrument.[76]

---

[66] Cal. Civ. Code § 1786.16(b) and (c).
[67] Cal. Civ. Code §§ 1786.20(d), 1786.50(a).
[68] Laws 2001, Ch. 720 (S.B. 168).
[69] Cal. Civ. Code § 1785.11.1(a).
[70] Cal. Civ. Code § 1785.11.1(f).
[71] Cal. Civ. Code § 1785.11.2(a).
[72] Cal. Civ. Code § 1785.11.2(b).
[73] Cal. Civ. Code § 1785.11.2(c).
[74] Cal. Civ. Code § 1785.11.3.
[75] Cal. Civ. Code § 1785.11.2(a), (h).
[76] Cal. Civ. Code § 1785.11.2(*l*)(1).

A consumer may allow his or her credit report to be accessed by a specific party, or period of time, by following certain procedures. The consumer may also request that a security freeze be removed.[77] The credit reporting agency may not charge a fee to a person who has been a victim of identity theft for placing, lifting, or removing a "security freeze."[78]

Social Security Numbers

Effective July 1, 2002,[79] a person or entity must not:

(1) Publicly post or publicly display in any manner an individual's social security number, that is, to intentionally communicate or otherwise make available to the general public an individual's social security number;

(2) Print on any card required for the individual to access products or services provided by a person or entity the individual's social security number;

(3) Require an individual to transmit his or her social security number over the Internet unless the connection is secure or the social security number is encrypted;

(4) Require an individual to use a social security number to access an Internet Website unless a password or unique personal ID number or other authentication is also required; or

(5) Print an individual's social security number on any materials that are mailed to the individual unless state or federal law requires it (applications and forms sent by mail may include the individual's social security number).[80]

A person or entity that has used, prior to July 1, 2002, an individual's social security number in a manner inconsistent with the foregoing may continue to use that number in the same manner if all of following conditions are met: (a) the use is continuous (if the use is stopped for any reason, the foregoing provisions apply); (b) the individual is provided an annual disclosure commencing in 2002 that informs the individual that he or she has the right to stop the use of his or her social security number in a manner prohibited by the foregoing; (c) a written request by an individual to stop must be honored within 30 days of request (no fee may be charged for this); and (d) the person or entity must not deny services to an individual because he or she requests the person or entity to stop using his or her social security number.[81]

A person or entity may use social security numbers of individuals for internal verification or administrative purposes, and may collect, use or release such numbers as may be required by state or federal law.[82]

---

[77] Cal. Civ. Code § 1785.11.2(a) – (g), (j).
[78] Cal. Civ. Code § 1785.11.2(m).
[79] Laws 2001, Ch. 720 (S.B. 168).
[80] Cal. Civ. Code § 1798.85(a).
[81] Cal. Civ. Code § 1798.85(c).
[82] Cal. Civ. Code § 1798.85(d).

Responsibilities of State and Local Agencies

The Information Practices Act of 1977 was recently amended to require state and local agencies to disclose to California residents a breach of security of the computerized data system where personal information is stored and which information is believed to have been acquired by an unauthorized person.[83] "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: Social security number, driver's license number or California identification card number, account number, credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.[84]

An agency that owns or licenses computerized data that includes personal information is required to disclose any breach of the security of the system following discovery or notification of the breach to any resident of California whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person.[85] Some elaborate procedures for notification are included in the law.

Federal Criminal Law

The provisions of Subtitle B of the Gramm-Leach-Bliley Act ("GLB") prohibit obtaining customer information by false pretenses, and are the real "teeth" in GLB. The provisions of Subtitle B of GLB, with its own set of rules, definitions and enforcement, are not very widely known.

Subtitle B of GLB provides that it is a violation of federal law for any person to obtain, or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed to any person, *customer information of a financial institution* relating to any other person –

(1) by making a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of a financial institution;

(2) by making a false, fictitious, or fraudulent statement or representation to a customer of a financial institution; or

(3) by providing any document to an officer, employee, or agent of a financial institution, knowing that the document is forged, counterfeit, lost, or stolen, was fraudulently obtained, or contains a false, fictitious, or fraudulent statement or representation.[86]

It is also a violation of federal law for a person to request of another person to obtain *customer information of a financial institution*, knowing that the person will obtain, or attempt to obtain, the information from the financial institution in any manner set forth above.[87]

---

[83] Laws 2002, Ch. 915 (S.B. 1386).
[84] New Cal. Civ. Code § 1798.29(e).
[85] New Civ. Code § 1798.29(a).
[86] 15 U.S.C. § 6821(a).
[87] 15 U.S.C. § 6821(b).

"Customer information of a financial institution" means any information maintained by or for a financial institution that is derived from the relationship between the financial institution and a customer of the financial institution and is identified with the customer.[88] The definition is different than the one provided for "nonpublic personal information"[89] under Subtitle A of GLB, in part because that definition reaches "consumers" and not just "customers." Another reason for the difference is that the "customer" under Subtitle B is *any* customer to whom the financial institution provides products or services, not just those that are "financial" in nature, and not just those in connection with personal, family or household purposes.[90] The limiting factor here is in the definition of "financial institution," which is much more narrow than that under Subtitle A of GLB. A "financial institution" means "any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust, or other financial account or relationship with the institution."[91] Certain financial institutions[92] are *specifically included* in this definition:

- A depository institution as defined in the Federal Reserve Act Section 19(b)(1)(A);[93]
- Any broker or dealer;[94]
- Any investment adviser;[95]
- Any investment company;[96]
- Any insurance company;
- Any loan or finance company;
- Any credit card issuer or operator of a credit card system; and

[88] 15 U.S.C. § 6827(2).
[89] "Nonpublic personal information" is "personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution." 15 U.S.C. § 6809(4)(A).
[90] The term "customer" is defined as any person, or authorized representative of a person, to whom the financial institution provides a product or service, including that of acting as a fiduciary. 15 U.S.C. § 6827(1). Note especially that the term is not limited to one in which the products or services involve personal, family or household purposes, nor is it limited strictly to "financial" products or services. Compare 15 U.S.C. § 6809(9).
[91] 15 U.S.C. § 6827(4)(A).
[92] The Federal Trade Commission is given the authority to prescribe regulations clarifying or describing the types of institutions that are to be treated as financial institutions for purposes of Subtitle B, but to date, such regulations have not been released.
[93] 12 U.S.C. § 461(b)(1)(A). The term "financial institution" does not include the Federal Agricultural Mortgage Corporation, or any entity chartered and operating under the Farm Credit Act of 1971. 15 U.S.C. § 1687(4)(D)
[94] "Broker" and "dealer" have the same meanings as given in the Securities Exchange Act of 1934, Section 3 (15 U.S.C. 78c). The term "financial institution" does not include any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act. 15 U.S.C. § 1687(4)(D).
[95] "Investment adviser" has the same meaning as given in the Investment Advisers Act of 1940, Section 202(a)(11) (15 U.S.C. 80b-2(a)).
[96] "Investment company" has the same meaning as given in the Investment Company Act of 1940, Section 3 (15 U.S.C. 80a-3).

- Any consumer reporting agency[97] that compiles and maintains files on consumers on a nationwide basis.[98]

The prohibitions in Subtitle B do not apply to law enforcement agencies that obtain customer information from a financial institution in connection with the performance of their official duties,[99] or to insurance institutions investigating insurance fraud.[100] The prohibitions also do not apply to prevent any state-licensed private investigator from obtaining customer information to the extent reasonably necessary to collect child support from a person adjudged to have been delinquent in his or her obligations by a federal or state court.[101] And of course, financial institutions testing their security procedures or systems for maintaining confidentiality of customer information, or investigating allegations of misconduct or negligence on the part of any officer, employee or agent of the financial institution, or of recovering customer information that was obtained in violation of the prohibitions are not prevented from obtaining customer information if it is for these reasons.[102]

Whoever knowingly and intentionally violates, or knowingly and intentionally attempts to violate these prohibitions will, upon conviction, be subject to fines in accordance with 18 United States Code Section 3571, which provides for both felony and misdemeanor fines, or imprisoned for not more than five years, or both.[103] Whoever violates, or attempts to violate these prohibitions while violating another law of the United States, or as part of a pattern of any illegal activity involving more than $100,000 in a 12-month period, will upon conviction of a felony be fined $500,000[104] and imprisoned for not more than 10 years, or both, if an individual, or fined $1,000,000[105] if an organization.

Various federal agencies are charged with administrative enforcement.[106] In the case of national banks and federal branches and federal agencies of foreign banks, the agency is the Office of the Comptroller of the Currency; in the case of member banks of the Federal Reserve System other than national banks, and branches and agencies of foreign banks (other than federal branches, federal agencies and insured state branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25A of the Federal Reserve Act, the agency is the Federal Reserve Board; in the case of banks insured by the Federal Deposit Insurance Corporation ("FDIC") (other than members of the Federal Reserve System and national nonmember banks) and insured state branches of foreign banks, the agency is the FDIC; in the case of savings associations the deposits of which are insured by the FDIC, the agency is the Office of Thrift Supervision; in the case of federally chartered credit unions, the agency is the National Credit

---

[97] "Consumer reporting agency" is defined in the Consumer Credit Protection Act, Section 603(p). (15 U.S.C. § 1681a(p)).
[98] 15 U.S.C. § 6827(4)(B).
[99] 15 U.S.C. § 6821(b).
[100] 15 U.S.C. § 6821(e).
[101] 15 U.S.C. § 6821(g).
[102] 15 U.S.C. § 6821(d).
[103] 15 U.S.C. § 6823(a).
[104] 18 U.S.C. § 3571(b)(3).
[105] 18 U.S.C. § 3571(c)(3).
[106] Each federal banking agency, the National Credit Union Administration, the Securities and Exchange Commissioner, and self-regulatory organizations, as appropriate, are to review regulations and guidelines under their respective jurisdictions, and are to prescribe such revisions as are necessary to ensure that financial institutions have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect activities prohibited under these provisions. 15 U.S.C. § 6825.

Union Administration;[107] and in all other cases, the agency is the Federal Trade Commission.[108] The FTC has begun to report prosecuting cases under this new scheme.

Another federal law, The Identity Theft and Assumption Deterrence Act of 1998,[109] amended provisions of and added subsections to the section of United States Code Title 18, Chapter 47, Fraud and False Statements, dealing with fraud and related activity in connection with identification documents and information.[110] Possessing, using, transferring or having a document-making implement that products false identification documents is unlawful.

Among other things, a person who knowingly transfers or uses a means of identification of another person with the intent to commit or to aid or abet any unlawful activity, whether a violation of federal law or that constitutes a felony under state or local law, is subject to a fine and imprisonment.[111] The identification is not limited to a document made or issued by the United States Government, such as a passport, but also covers personal identification data, such as name, social security number, date of birth, driver's license or personal identification card, unique biometric data such as fingerprint, voice print, retina or iris image or other unique physical representation, or an electronic identification number or address.[112]

If the false identification is used to obtain anything of value worth $1,000 or more during any one-year period, the prison time is up to three years.[113] If the false identification is used to facilitate drug trafficking or a crime of violence, or following a prior conviction under this section, the prison time goes up to 20 years.[114] If the false identification is used facilitate an act of international terrorism, the prison time goes up to 25 years.[115]

Federal Trade Commission's ID Theft Tool

In an effort to assist individuals to fight against identity theft and restore their credit files, the Federal Trade Commission ("FTC") unveiled in February 2002 an effective do-it-yourself tool. An individual may use the "ID Theft Affidavit" – a model form that the individual can complete – to alert companies and credit reporting agencies to the fraudulent activity on an account or loan committed by the thief. The ID Theft Affidavit is accepted by participating creditors, retailers, banks and other financial institutions. The form is available at www.consumer.gov/idtheft/affidavit.htm or by calling telephone number 1-877-ID-THEFT.

OCC Bulletin on Identity Theft

The Office of the Comptroller of the Currency has released a bulletin directing consumers on steps to take when their personal information has been stolen. The bulletin provides helpful tips on protecting against identity theft, phone numbers, and definitions. The bulletin is available at www.occ.treas.gov.

---

[107] 15 U.S.C. § 6822(b).
[108] 15 U.S.C. § 6822(a).
[109] P.L. 105-318, 112 Stat. 3007 (Oct. 30, 1998).
[110] 18 U.S.C. § 1028.
[111] 18 U.S.C. § 1028(a)(7).
[112] 18 U.S.C. § 1028(d)(4).
[113] 18 U.S.C. § 1028(b)(2).
[114] 18 U.S.C. § 1028(b)(3).
[115] 18 U.S.C. § 1028(b)(4).

Other Useful Websites

The California Department of Consumer Affairs has one of the more useful and complete websites offering information and assistance in connection with identity theft. Go to www.privacyprotection.ca.gov.

Record Retention and Destruction Guidelines to Safeguard Customer Records

Pursuant to the federal "Safeguards Rule" adopted under GLB,[116] many financial institutions have made their business records retention and destruction procedures part of their written information security programs. An "information security program" is "the administrative, technical, or physical safeguards that a financial institution uses to access, collect, process, store, use, transmit, dispose of, or otherwise handle customer information."[117]

One of the elements of an information security program is that the financial institution must "identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks."[118] Another element is that once identified, a financial institution must design and implement information safeguards to control those risks, and regularly test and monitor the effectiveness of the controls.[119]

Effective January 1, 2001, Sections 1798.80 through 1798.82 were added to California's Civil Code[120] to require that a business[121] ensure the privacy of a customer's[122] personal information, as defined, contained in records. A business must take all reasonable steps to destroy, or arrange for the destruction of a customer's records[123] within its custody or control containing personal information which is no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.[124]

"Personal information" means any information that identifies, relates to, describes, or is capable of business associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone

---

[116] Sections 501 and 505(b)(2) of GLB; Joint Agencies Rule, 66 Fed. Reg. 8616 (Feb. 1, 2001); FTC Rule, 67 Fed. Reg. 36484 (May 23,2002).
[117] FTC Safeguards Rule 16 CFR § 314.2(c).
[118] FTC Safeguards Rule 16 CFR § 314.4(b).
[119] FTC Safeguards Rule 16 CFR § 314.4(c),
[120] Laws 2000, ch. 1039, A.B. 2246.
[121] "Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized to operate at a profit, including a financial institution, organized, chartered, or holding a license or authorization certificate under the law of the State of California, any other state, the United States, or of any other country or the parent or the subsidiary of a financial institution. Cal. Civ. Code § 1798.80(a).
[122] "Customer" means an individual (natural person) who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business. Cal. Civ. Code § 1798.80(c).
[123] "Records" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted. "Records" does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address and telephone number (*e.g.*, telephone books). Cal. Civ. Code § 1798.80(b).
[124] Cal. Civ. Code § 1798.81.

number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information.[125]

Any customer injured by a violation of this title may institute a civil action to recover damages. Any business that violates, proposes to violate, or has violated this new law may be enjoined.[126]

Effective July 1, 2003, the responsibilities of businesses under these provisions are *significantly* expanded.[127] The legislative intent of the new law is edifying:

> Section 1. (a) The privacy and financial security of individuals is increasingly at risk due to the ever more widespread collection of personal information by both the private and public section.
>
> (b) Credit card transactions, magazine subscriptions, telephone numbers, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports and Internet Web sites are all sources of personal information and form the source of material for identity thieves.
>
> (c) Identity theft is one of the fastest growing crimes committed in California. Criminals who steal personal information such as social security numbers use the information to open credit card accounts, write bad checks, buy cars, and commit other financial crimes with other people's identities. The Los Angeles County Sheriff's Department reports that the 1,932 identity theft cases it received in the year 2000 represented a 108% increase over the previous year's caseload.
>
> (d) Identity theft is costly to the marketplace and to consumers.
>
> (e) According to the Attorney General, victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information in imperative.[128]

Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information,[129] must disclose any breach of the security of the system[130] following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible

---

[125] Cal. Civ. Code § 1789.80(e).
[126] Cal. Civ. Code § 1798.92(a) and (b).
[127] Laws 2002, Ch. 915 (S.B. 1386).
[128] *Id.*
[129] As used in this section, "personal information" means an individual's first name or fist initial and last name in combination with any one or more of the following data elements, when either the name of the data elements are not encrypted: Social security number, driver's license number of California identification card number, account number, credit or debit number, in combination with any required security code, access code or password that would permit access to an individual's financial account. New Cal. Civ. Code § 1798.82(e).
[130] A "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. New Cal. Civ. Code § 1798.82(d).

and without unreasonable delay, consistent with the legitimate needs of law enforcement,[131] or [consistent with] any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.[132] An elaborate procedure for notification is provided in the new law.[133]

Any person or business that maintains computerized data that includes personal information that the person or business does not own must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[134]

Conclusion

California identity theft law most certainly, and federal law most probably, will continue to expand in the coming years. Many of these provisions have the prospect of protecting against and aiding victims of identity theft; unfortunately, without more care being given, it is possible that some of these new laws will simply mire creditors and credit reporting agencies in hyper-technical regulation without producing the salutary effect needed.

Elizabeth A. Huber, Esq.
Hudson Cook, LLP
El Segundo, California
Telephone 310-536-9099
Email: ehuber@hudco.com

* * * * * * *

[131] The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. New Cal. Civ. Code § 1798.82(c).
[132] New Cal. Civ. Code § 1798.82(a) effective July 1, 2003; existing Cal. Civ. Code § 1798.82 is renumbered new Civ. Code § 1798.84.
[133] *See* new Cal. Civ. Code § 1798.82(g).
[134] New Cal. Civ. Code § 1798.82(b).